General Data Protection Regulations (GDPR)
Data Protection Policy

1. Introduction

Yalding Parish Council (YPC) recognises its responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The Council is committed to protecting the privacy and security of all personal data it processes, whether relating to residents, service users, Councillors, staff, contractors or any other individuals.

Personal data means any information relating to an identifiable person, including names, addresses, email addresses, telephone numbers and any other information that can identify an individual.

The Council is registered with the Information Commissioner's Office (ICO).

2. Scope

This policy applies to all personal data processed by YPC in any format, including:

- Residents and members of the public
- Volunteers
- Councillors
- Contractors and suppliers
- Staff and job applicants
- Any other individuals whose data The Council processes

It applies to all Councillors, employees, volunteers and contractors who handle personal data on behalf of The Council.

3. Roles and Responsibilities

- The Clerk is The Council's Data Protection Lead and is responsible for overseeing compliance, maintaining records and responding to data protection queries.
- Councillors and staff must follow this policy and handle personal data securely and lawfully.
- Contractors and third processors must comply with data protection requirements through appropriate written agreements.

4. Data Protection Principles

YPC will ensure that personal data is:

- **Processed lawfully, fairly and transparently**

  Individuals will be informed about how their data is used through The Council's Privacy Notice.

- **Collected for specified, explicit and legitimate purposes**

  Data will only be used for the purpose for which it was collected.

- **Adequate, relevant and limited to what is necessary**

  Only the minimum amount of data required for The Council's functions will be collected and retained.

- **Accurate and kept up to date**

  Inaccurate data will be corrected or deleted promptly.

- **Kept for no longer than necessary**

  Data will be retained in accordance with The Council's Retention Schedule and securely destroyed when no longer required.

- **Processed securely**

  Appropriate technical and organisational measures will protect data from loss, unauthorised access or misuse.

5. Lawful Bases for Processing

The Council will ensure that all processing is based on one or more lawful bases under Article 6 UK GDPR, typically:

- Public Task – most council functions
- Legal Obligation – finance, audit, transparency requirements

- Contract – service agreements
- Consent – mailing lists, photographs, optional communications
- Vital Interests – rare, emergency situations
- Legitimate Interests – only where appropriate and not overridden by individual rights

YPC does not routinely process special category data. If such information is received unexpectedly it will only be processed where an additional lawful condition applies.

Special category data is personal data that is more sensitive and requires extra protection. It includes information about an individual's such as:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- health
- sex life or sexual orientation
- genetic or biometric data used for identification

6. Data Security

The Council will ensure that:

- Personal data stored electronically is password protected and accessible only to authorised users
- Paper records are kept securely in locked storage
- Councillors and staff use secure email practices
- Personal devices used for council business follow the Council's IT Security Policy
- Data is backed up and protected against loss or damage

7. Data Protection Impact Assessments (DPIAs)

DPIA is a process that helps The Council identify and minimise data protection risks when carrying out activities that may have a high impact on individuals' privacy. DPIAs are required under UK GDPR where processing is likely to result in a high risk to people's rights and freedoms. Examples of activities that may require a DPIA include large scale monitoring, new technologies or processing that involves special category data.

YPC does not routinely carry out high risk processing. The only activity that may require a DPIA is the operation of CCTV, which is covered in a separate CCTV Policy. If The Council introduces any new systems or services that could affect privacy, it will assess whether a DPIA is required and complete one where necessary.

8. Data Sharing and Third-Party Processors

Personal data may be shared with third parties where necessary and lawful, including:

- Internal and external auditors
- Contractors providing services to The Council
- Government bodies where legally required

Any third party processing data on behalf of The Council must have a written agreement ensuring compliance with data protection law.

The Council will never sell personal data.

9. International Data Transfers

The Council will only transfer personal data outside the UK where lawful safeguards are in place to protect individuals' rights. These safeguards may include adequacy regulations, standard contractual clauses or other mechanisms approved under UK data protection law. YPC currently uses Dropbox for limited data storage. The Council will ensure that any cloud based service used has suitable protections in place before personal data is stored or processed within it.

10. Individual Rights

Individuals have the following rights under UK GDPR:

- Right of access (Subject Access Request)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to object
- Right to data portability (rarely relevant to councils)

Requests will be handled in accordance with The Council's Subject Access Request Policy.

11. Data Breaches

All data breaches, whether accidental or deliberate, must be reported immediately to The Clerk.
The Council will:

- Investigate all breaches
- Record them in the breach log
- Assess whether they must be reported to the ICO within 72 hours
- Notify affected individuals where required

This process is detailed in the Council's Data Breach Policy.

12. Retention and Disposal

Personal data will be retained only for as long as necessary and in line with The Council's Retention Schedule. Data that is no longer required will be securely shredded or permanently deleted.

13. Privacy Notice

The Council's Privacy Notice explains to the public how their data is used, their rights and how to contact The Council about data protection matters. This policy should be read alongside the Privacy Notice.

14. Training and Awareness

Councillors, staff and volunteers handling personal data will receive appropriate training and guidance to ensure compliance.

Adopted on: 03 March 2026

To be reviewed annually at the Annual Parish Council Meeting (See Minutes of that meeting)